THE BUSINESS-LED ACCREDITOR - OR....

HOW TO TAKE RISKS AND SURVIVE

Michael E J Stubbings
Room A/1411,
Government Communications Headquarters,
Priors Road,
CHELTENHAM
Gloucestershire
GL52 5AJ
United Kingdom
Tel: +44-1242-221491 ext 3273

What The Accreditor Does - But Shouldn't

The computer security accreditors inspect a new computer system. They have previously gone through System Security Policies (or Plans) with a fine-tooth comb. They have ensured that every 'i' is dotted and every 't' crossed. They have put their feet down with firm hands all the way through the project - with semantic contortions to match. The system manager is on his best behaviour - with all the more troublesome users sent on leave for the day. Sample audit trails are available containing evidence of carefully staged 'security-related' events. The accreditors prowl around the system, looking stern, as is expected of them. And then a certificate is signed - the system is now accredited: it meets the rules. Everyone is happy.

What have we achieved? Time is money, and we have spent a lot of it in giving this system its certificate. We may well have bought hardware or software products solely to satisfy the rules. We are likely to have imposed ways of working on the user community which they would otherwise not have implemented. We now know that this system, its operating and configuration control procedures, all meet the rules. Which is what the accreditors have traditionally been for - to ensure that systems meet the rules.

This approach has a number of advantages. These include:

a) Clarity: everyone knows where they stand. Systems either meet the rules or they don't.

b) Documents: In the USA the Orange Book, and in the UK, the CESG (Communications and Electronics Security Group) Memoranda give all the guidance necessary.

c) Training: Low training costs, as rules are easier to teach than judgement.

d) Culture: This approach fits well with traditionally rule-based or hierarchical environments.

Life being what it is, there are some disadvantages. These include:

a) Support: A large infrastructure of developers, evaluators and accreditors is needed to support this approach.

b) Perception (1): Security is perceived to be a hurdle - no sense of local 'ownership'.

c) Perception (2): No perception of accreditation as an instrument for obtaining business advantage, i.e. value for money.

d) Costs and Benefits: Rules and procedures do not reflect the value of the assets (systems or data) to the organization, nor the costs of the different sorts of security breach.

e) Value: No definition of 'value'.

To this I would add a few personal observations. I was for many years a system and project manager - on the receiving end of the accreditors' ministrations. In November 1993 I became the senior computer security accreditor, at just about the same time that a new head of computer security was appointed - my immediate boss. Apart from the above, we both noticed that:

a) Accreditors (expensive people) spend most of their time at their desks reviewing documents.

b) Whenever an accreditor spoke to a system or project manager, it was usually to tell them that they had done something wrong.

c) There was distrust, suspicion, and occasionally open (and verbally robust) hostility between accreditors and system/project staff.

d) In an increasingly value-driven environment, the concept of justifying imposed security costs did not exist. Some of the measures we imposed did not add anything to a system's security profile. They were imposed because the rule book (or custom and practice) said they must be imposed.

e) Neither end-user objectives nor system functionality (that is, the system's value to the organization - its business case) had any place in the accreditation process.

f) Accreditors were overworked to the point that individuals were suffering, and there was an increasing danger that systems with real security problems were being 'lost in the noise'. Conversely, most systems and projects presented very few real problems (as opposed to theoretical ones).

g) The commercial environment was talking about risk management; about quantifying and assessing risk. We didn't normally use the word 'risk'.

Of course, a lot of us *do* use that word, but how many of us find out the risk to a system by looking it up in a table? How many of us go on to minimise that risk by looking up a series of measures in another table? And how does that help us to know the actual vulnerabilities of our systems rather than the theoretical ones? How does that help us to assure our organizations that we are causing money to be spent wisely? That is the starting point for the GCHQ (Government Communications Headquarters) approach. Although we are in the public sector, we no longer believe that we can go to our financial planners, or to our project fund holders and say ‘Spend *x* thousand pounds or dollars, or *x* project hours because we say so - trust us, we’re professionals’. That isn’t good enough, and rightly so. It’s not an approach I would like to try getting past a shareholders’ meeting or a public accounts committee.

The New UK Government Security Philosophy

At about the same time that my boss and I moved into the accreditation world, the United Kingdom Cabinet Office (similar in some ways to the various Presidential offices) issued the Review of Protective Security (RPS). This document, formally announced in Parliament by the Prime Minister, mandated a new approach throughout government service. It covered a wide range of security considerations, setting out a philosophy which changed the whole basis upon which security professionals approached their jobs. The subjects included personnel vetting, paper controls, and a range of other matters, including IT Security. It comes down to one thing. In the past we did our best to avoid risks. Now we manage them.

The background to this approach is basically what I have already been describing. Her Majesty’s Government (HMG) demands value for money from its officials. Civil Servants should not spend - or allow to be spent - money which does not add something to the value of the product. Value is defined as the extent to which the product furthers the business objectives of the organization. Is security one of the organization’s business objectives? In the case of my own department, the answer is most definitely ‘Yes’. In other departments, particularly those holding information about individual people (e.g. Social Services, Agriculture or other ministries), the answer will also be ‘Yes’. Once accepted as a business objective, security becomes the responsibility of the organization, and everyone in it, not simply the preserve of people seen often as ‘those professional obstacle-makers and blame-distributors in the security department’. Sometimes we are even viewed as the people employed to *take* the blame for security problems.

The other result of this approach is that security funding has to have a business case made for it, in competition with all the other requirements for spending. This is as it should be. Perhaps a particular security measure is essential to the survival of the organization. Perhaps the cost of not implementing that measure is outweighed by the benefits of using the funds elsewhere. *Security spending is primarily a management matter, not a technical one*. If the organization gains no significant benefit from a security measure, why spend time and money on it? And if you are spending time, then you are also spending money. Those of you who work for commercial organizations will be very familiar with this approach. It has not, until now, been part of the government culture in the UK. I suspect that this vocabulary will not be entirely unfamiliar to those in US government service.

So, the idea had come of age. Government policy and our own internal observations coincided in both timing and content, and we had a marvellous opportunity to rethink our whole approach to IT security and to accreditation. We were not the first in the field (if you will excuse the pun) - the United Kingdom’s Ministry of Agriculture, Fisheries and Food (MAFF) preceded us with an added-value philosophy - not that I knew it at the time. We didn’t stop with IT. What I am about to describe was carried on within a total rethink of the functions and tasks of an internal security division. IT Security does not exist in a vacuum; it shares an environment with paper-handling, personnel, training, and procedural security measures. If there isn't a common philosophy for all of these, with an obvious relationship to the organization's culture and shared objectives, security measures become discredited, circumvented and imposed only by force. Under those circumstances, no-one wins.

What We Did

We didn't call it Business Process Re-engineering, but that's basically what we were doing. We took the RPS philosophy, and looked for the core processes which would further GCHQ's business objectives, and defined what contribution those processes would make. We then set about designing a structure and set of procedures which would implement these processes with the greatest economy and efficiency - in other words achieving the maximum value for money. I'm not going to describe the way we went about doing this, save to mention that we involved our client community - GCHQ's project, system and security managers. Many interviews were carried out, and it was interesting to note that the observations noted earlier were largely consonant with what our clients were saying. The one quotation which sticks in my mind is that the computer security branch staff were 'A bunch of computer illiterates with a six-inch rulebook'. We are not that, and never were, but it shows the extent to which people on both sides of the accreditation/project divide had stopped listening to each other - if they had ever started. The fact that our clients had said that about us showed that regardless of the RPS, something had gone seriously wrong.

What We Ended Up With

At the end of all this soul-searching, we came up with a set of principles, an environment for them, and tools with which to apply them. Part of the environment was a 'given' - the physical nature of the GCHQ campus, the physical and logical aspects of the department's existing telecommunications, the law of the land, and the policies of HMG. Most of the rest was open to us to reshape as we saw fit - and we did.

The Principles

Our principles are unlikely to come as a surprise to anyone; they came directly from the RPS philosophy and from our own observations.

a) IT security is the direct and accountable responsibility of the system users and managers, it being by definition part of their overall security profile and therefore one of their own business objectives - an idea often abbreviated to the concept of 'local ownership'.

b) The accreditor's job is to assist project and system staff to identify, document and accommodate their own security risks and requirements, where by definition these include GCHQ's corporate requirements, and then to certify if they have been met.

c) The actual provision of IT security features and procedures is *not* the accreditor's job.

d) Each security measure must add value to the system, where value means that the cost of the measure is exceeded by the consequent business benefits. Accreditors must therefore identify security-related proposals which are not cost-effective, with a view to their removal.

e) Security costs include impediments to convenient use, limitations to desired functionality, security and system administration overheads, and the costs of extra hardware, software or maintenance contracts.

f) It is essential that IT security staff are available as advisors to system managers and their users throughout the life of the system.

g) It is essential that the organization has some assurance that despite the move away from rule-based accreditation, appropriate and cost-effective corporate standards are identified, adhered to, and kept under periodic review.

The Environment

I have already alluded to the 'given' nature of part of GCHQ's environment. A particular set of site access rules, security patrols, personnel clearance policies etc. were already in place. For obvious reasons I am not going to describe these: suffice to note that the existence of a well-established and reliable campus-wide regime allowed us more flexibility in the construction of our procedures than might otherwise have been the case. I would add that the TEMPEST profile and risk assessment associated with the two GCHQ sites in Cheltenham is an important factor in defining the environment within which we operate.

Aspects of the environment which were open to adjustment and renewal included our own structures, staffing, job descriptions and internal IT resources. When we went into this process, we had one senior computer security accreditor (me) with five assistants. Two of my staff concentrated largely on collaborative projects, i.e. those where GCHQ's internal policies did not apply because of the involvement of other agencies such as the Armed Forces. There were, in addition, 2 Computer and Communications Security policy staff who for historical reasons undertook various infrastructure and communications accreditation tasks. When considering our structure, we also had to bear in mind the wider security division reorganization which I mentioned earlier. As it happened, the two programmes dovetailed nicely, and the new structure reflects the requirements of both.

Our New Structure

We redeployed one accreditor to lead a Computer and Communications Security Monitoring Team, and recruited two assistants for her. They have a two-fold job. The first is to carry out a security inspection of each area in the department, such that everyone can expect an inspection every 2-3 years. The scope of each visit is all staff, systems and procedures operating under a particular security management regime. That usually means one open-plan office, or a contiguous group of offices or laboratories. The visits are intended to be advisory in manner, so that they can work with staff to enhance their security effectiveness, rather than coming in as a police force trying to catch people out. Naturally, disciplinary procedures are available to deal with wilful disregard of security measures, but we are not interested in pursuing people for honest mistakes and misunderstandings. We would rather sit down with them and help them to improve matters - for the sake of their own, and therefore corporate, effectiveness. The Monitoring

Team's job is to ensure that systems continue to be configured and operated in a manner reflecting their declared and approved security profiles.

The second role for the Monitoring Team is as an incident response office. Should a suspicious IT security event be noted, it will be investigated first by local staff, who are obliged to call in the Team if a satisfactory explanation is not immediately forthcoming. Team members have a wide variety of resources to call upon to support them. These include the accreditors, the department's own technical experts, staff from other security disciplines, and members of the Communications and Electronics Security Group (CESG). CESG is the UK national authority for communications and computer security matters, setting guidelines for all government systems. They are collocated with, but separate from, GCHQ. It is broadly similar to the USA's NSA/ISSO organization. At the time of writing, we are considering the possibility of seeking liaison membership of FIRST (Forum of Incident Response and Security Teams) for our Monitoring Team.

The Monitoring Team coordinates closely with the Internal Audit Unit. Each acts as a specialist adviser for the other, and they take care that their respective inspection programmes do not clash. Reports from each are made available to the other, insofar as personnel and management data release considerations permit this. In practice, such factors should rarely apply.

All other computer and communications accreditation work (including that previously carried out by the policy staff) is now handled by the remaining four accreditors, plus myself. What might have been an unmanageable increase in workload is assuaged by a change in procedures limiting the amount of attention given to routine systems. This procedural change is described in more detail below. I am using this opportunity to redefine my own work pattern in order to devote time to more general topics such as defining a security profile for a GCHQ Corporate Web (that is, one most definitely *not* connected to The Internet). The two policy staff are moving into a dedicated policy unit serving the interests of all the security disciplines. As and when IT Security policy issues arise they will coordinate task-orientated teams drawing on, among others, staff from the accreditation and monitoring teams.

The two teams are located in adjacent offices - with an open door between them. They share IT resources, including system databases, and a common office automation environment. Both teams report to the same senior manager. It is our intention that a close working relationship should continue between the two groups.

The Tools

Our experience and measurements led us to believe that something like 75% of the incoming accreditation workload related to systems which either presented no real security threat, or were operating in arenas where appropriate security profiles had already been defined. It therefore made little sense for accreditors to handle each system individually. In order to reflect this, and to implement the principles defined earlier, we decided to put all systems into one of two categories: routine and exceptional.

Routine Systems

These systems are the 75% just mentioned. They operate within a clearly defined security profile. This profile includes the system's location, the classification (or protective marking as we say in the UK) of its software and data, the clearance level of its users and managers, and its connections. A flowchart was drawn up to guide system and project managers to a decision as to whether or not their systems fell within this profile. For those which do, a campus-wide document set was written, comprising Baseline Security Measures, department-wide Security Operating Procedures (aimed at system and security managers), and a department-wide Secure Features User's Guide (aimed at the normal user). These are all very short documents, setting out the security objectives in functional terms, plus the responsibilities of individual members of staff. These include responsibilities for configuration and change control, system management procedures, and also define the circumstances under which reaccreditation would be required. Project and system managers wishing to have a system accredited are asked to confirm in writing that they accept and can implement the measures described in these documents. If so, they register their systems with the accreditors. The system is then entered into the Monitoring Team's visits programme, and an accreditation certificate is issued. For the first six months of this new way of accrediting systems (starting January 1996), the Monitoring Team will in fact inspect every routine system, in order to verify whether or not the new methods are working effectively. As I said earlier, systems needing attention were in danger of being lost 'below the noise'. The introduction of a 'routine system' accreditation track will reduce the noise level to a point where we can handle the systems which would most benefit from our attention.

Exceptional Systems

That leaves the systems which are 'interesting'. These continue to be handled in the classical manner, for the most part with a tailored document set, considerable accreditor involvement at all stages of the project, and a detailed post-installation inspection. It is, of course, open to the accreditor to use any of the routine system document elements should they be deemed suitable. Some systems will be exceptional for reasons connected more closely with administrative considerations rather than security ones. I anticipate an increasing level of formality when holding commercial data - you may remember the presentation last year entitled 'The Development of Generally-Accepted System Security Principles', which addressed this issue among others. Other systems will present problems, where some new balance of procedural, technical and personnel controls has to be found in order to achieve a satisfactory security profile. Perhaps money has to be spent, perhaps the functionality has to be redefined, perhaps the accommodation needs to be altered. Maybe it's a simple matter of adjusting the system configuration. In all of these considerations, the accreditor has to find the appropriate cost/benefit balance. Once this balance is found, an exceptional system will usually be inspected by the accreditor, possibly in the company of a member of the Monitoring Team. It will then be entered into their continuing inspection programme.

Summary

Rule-based, predominantly technical, computer and communication security measures are no longer a cost-effective response to the security requirements of a modern organization, whether in government, commerce or in industry. If an organization has inadequate security, its business effectiveness is impaired and its survival threatened. If an organization has too much security, it is wasting resources. That too will limit its business effectiveness and threaten its survival. Security must make its case for a slice of the corporate cake along with all the other business activities, and it must make its case on the basis of its contribution to the overall well-being of the organization. Security is first, last and always a management matter, whether the management is at the level of a national government, or the board of directors of a small company.

Technical measures exist only to implement business objectives effectively, at minimum cost. This is what GCHQ has sought to implement using the mechanisms outlined in this paper. At the time of writing (early February), we have just implemented the change, and we think we have got it just about right. By the time of the 1996 Conference, we will know for certain. I suppose I'm therefore taking a risk by submitting this paper in advance of a settling-in period. Still, risk management is what it's all about.